

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2005 年 7 月 21 日 (21.07.2005)

PCT

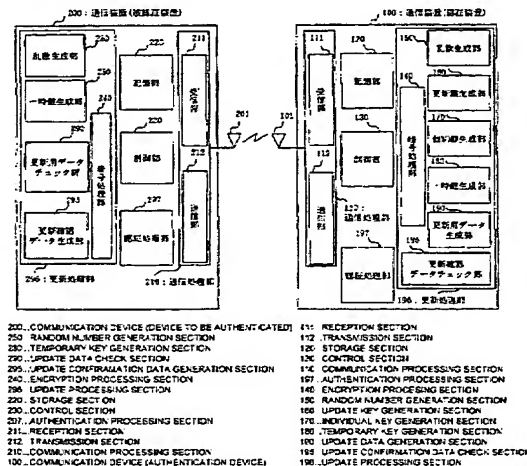
(10) 国際公開番号
WO 2005/067200 A1

- (51) 国際特許分類⁷: H04L 9/32, 9/14 (72) 発明者; および
(21) 国際出願番号: PCT/JP2004/005879 (75) 発明者/出願人 (米国についてのみ): 大越 文弘
(22) 国際出願日: 2004 年 4 月 23 日 (23.04.2004) (OHKOSHI, Takehiro) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目 2 番 3 号 三菱電機株式会社
(25) 国際出願の言語: 日本語 社内 Tokyo (JP). 山田 敬喜 (YAMADA, Keiki) [JP/JP];
(26) 国際公開の言語: 日本語 〒1008310 東京都千代田区丸の内二丁目 2 番 3 号 三菱電機株式会社 社内 Tokyo (JP). 牧田 覚 (MAKITA, Satoru) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目 2 番 3 号 三菱電機株式会社 社内 Tokyo (JP).
(30) 優先権データ: 特願 2003-432447
2003 年 12 月 26 日 (26.12.2003) JP (74) 代理人: 溝井 章司 (MIZOI, Shoji); 〒2470056 神奈川県鎌倉市大船二丁目 1 7 番 1 0 号 N T A 大船ビル
3 階 溝井国際特許事務所 Kanagawa (JP).
(71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI KAISHA) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目 2 番 3 号 Tokyo (JP). (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR,

(続葉有)

(54) Title: AUTHENTICATION DEVICE, DEVICE TO BE AUTHENTICATED, AND KEY UPDATE METHOD

(54) 発明の名称: 認証装置及び被認証装置及び鍵更新方法



(57) Abstract: An authentication device (100) includes: an authentication processing section (197) for performing authentication of a communication device (200) by using an authentication key; and an update key generation key section (160) for generating a new authentication key when the communication device (200) does not have an authentication key to be used for the authentication processing by the authentication processing section (197) and generating a new authentication key for updating the authentication key when the communication device (200) has an authentication key but authentication of the communication device (200) by the authentication processing section (197) has failed. By using the new authentication key generated by the update key generation section (160), the authentication processing section (197) again performs authentication of the communication device (200).

(57) 要約: 認証装置 100 に、認証用鍵を用いて通信装置 200 との間で認証処理をおこなう認証処理部 197 と、上記認証処理部 197 による認証処理に用いる認証用鍵を通信装置 200 が保持していない場合に新たな認証用鍵を生成し、上記通信装置 200 が保持している場合で上記認証処理部 197 による通信装置 200 との間での認証処理が失敗した場合に上記認証用鍵の更新のために新たな認証用鍵を生成する更新鍵生成部 160 とを備え、上記認証処理部 197 は、上記更新鍵生成部 160 によ

(続葉有)



BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG,

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。